EXAMINER 'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Pedro F. Suarez on 07-16-2010.

The application has been amended as follows:

In the claims:

Claims 9-11, 36, 39-41, and 46-47 are canceled.

6. (Currently Amended) A method, comprising:

determining, in a first network, an address associated with a called party of a second network, wherein the address is included in a session initiation protocol request;

determining based on said address if said called party is in a trusted network, wherein the determining if the called party of the second network is in a trusted network comprises checking if the address is contained in a database of trusted networks, wherein the database is provided in at least one of a serving call session control function and a security gateway, and wherein the database is in the first network; and

controlling a communication between the called party and a calling party of the first network based on whether said called party of the second network is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party

of the second network is not in the trusted network, the controlling comprises modifying the at least one message, wherein the controlling is performed by at least one processor.

7. (Currently Amended) A method, comprising:

determining, in a first network, an internet protocol address associated with a called party of a second network;

determining based on said internet protocol address if said called party of the second network is in a trusted network, wherein the determining if the called party is in a trusted network comprises checking if the internet protocol address is contained in a database in the first network of trusted internet protocol multimedia subsystem networks, wherein said database comprises domain names associated with the trusted internet protocol multimedia subsystem networks and internet protocol addresses of the trusted internet protocol multimedia subsystem networks, wherein if a determination is made that the internet protocol address is contained in the domain names, the called party is assumed to be in a trusted network; and

controlling a communication between the called party and a calling party of the first network based on whether said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network the controlling compromises modifying the at least one message, wherein controlling is performed by at least one processor.

37. (Currently Amended Presented) An apparatus, comprising:

a first determiner configured to determine an address associated with a called party located in another network, wherein the address is included in a session initiation protocol request;

a second determiner configured to determine, based on said address, if said called party of the another network is in a trusted network, the second determiner being configured to check if the address is contained in a database of trusted networks, wherein said database comprises domain names associated with the trusted networks and internet protocol addresses of the trusted networks, wherein if a determination is made that the address is contained in the domain names, the second determiner is further configured to assume that the called party is in a trusted network; and

a controller configured to control communication between the called party and a calling party, located in a network where the apparatus is located, based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified, wherein the database is located in the network.

53. (Currently Amended) A method comprising:

determining, at a serving call session control function in an internet protocol multimedia subsystem network, a trust relation with a called party in another network, wherein the determining if the called party of the another network is in a trusted relationship comprises checking whether an address, included in a session initiation protocol request, is contained in a database of trusted networks provided in at least one of a serving call session control function

and a security gateway, wherein the address is associated with the called party in the another network, wherein the database is located in an internet protocol multimedia subsystem network; and

controlling a communication of a message to the called party based on the determination, wherein if the called party is not trusted, the call session control function removes identity information relating to the calling party from the message, and if the called party is trusted, said identity information is retained, wherein controlling is performed by at least one processor.

Reason for Allowance

2. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 6, and 18, the prior art fails to teach or suggest a method, comprising a step of determining based on the address if the called party is in a trusted network, wherein the determining if the called party of the second network is in a trusted network comprises checking if the address is contained in a database of trusted networks, wherein the database is provided in at least one of a serving call session control function and a security gateway, and wherein the database is in the first network, in combination with other limitations, as specified in the independent claim 6.

Regarding claims 7 and 19, the prior art fails to teach or suggest a method, comprising a step of determining based on the internet protocol address if the called party of the second network is in a trusted network, wherein the determining if the called party is in a trusted network comprises checking if the internet protocol address is contained in a database in the first network of trusted internet protocol multimedia subsystem networks, wherein the database

comprises domain names associated with the trusted internet protocol multimedia subsystem networks and internet protocol addresses of the trusted internet protocol multimedia subsystem networks, wherein if a determination is made that the internet protocol address is contained in the domain names, the called party is assumed to be in a trusted network, in combination with other limitations, as specified in the independent claim 7.

Regarding claim 37, the prior art fails to teach or suggest an apparatus, comprising: a second determiner configured to determine, based on the address, if the called party of the another network is in a trusted network, the second determiner being configured to check if the address is contained in a database of trusted networks, wherein the database comprises domain names associated with the trusted networks and internet protocol addresses of the trusted networks, wherein if a determination is made that the address is contained in the domain names, the second determiner is further configured to assume that the called party is in a trusted network, in combination with other limitations.

Regarding claim 53, the prior art fails to teach or suggest a method comprising a step of determining, at a serving call session control function in an internet protocol multimedia subsystem network, a trust relation with a called party in another network, wherein the determining if the called party of the another network is in a trusted relationship comprises checking whether an address, included in a session initiation protocol request, is contained in a database of trusted networks provided in at least one of a serving call session control function and a security gateway, wherein the address is associated with the called party in the another network, wherein the database is located in an internet protocol multimedia subsystem network, in combination with other limitations.

3. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Duc Ho whose telephone number is (571) 272-3147. The examiner can normally be reached on Monday through Thursday from 7:30 am to 6:00 pm.

If attempt to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Patel, can be reached on (571) 272-2988.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-2600.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

5. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Patent Examiner
/DUC C HO/
Primary Examiner, Art Unit 2465
07-16-2010